Implementasi Kriptografi Teks pada SMS Menggunakan Algoritme *Multiple Encryption* dengan Metode RSA dan 3DES

Suci Indah Febriani[#1], Safitri Juanita[*2], Mardi Hardjianto[#3]

#Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur

**Program Studi Sistem Informasi, Fakultas Teknologi Informasi, Universitas Budi Luhur*

Jl. Ciledug Raya, Petukangan Utara, Jakarta Selatan, DKI Jakarta, 12260, Indonesia

[1]suciindahfebriani@gmail.com

[2]safitri.juanita@budiluhur.ac.id

[3]mardi.hardjianto@budiluhur.ac.id

Abstract*— *A short message service is a communication medium that is more preferred than voicemail. Currently, many people still use SMS because they have no platform or technology barriers, so the delivery is also fast. If you use a short message application, such as Whatsapp, it requires an internet connection. The sending of SMS contains important and confidential information. One example is the message about the time and place for drug raids or gambling. The problem is the security of information sent via SMS is quite vulnerable to information leakage. Therefore, an application is needed to secure these text messages from being read by unauthorized parties. This security uses multiple encryption with the Rivest Shamir Adleman (RSA) cryptographic algorithm and the Triple Encryption Data Standard (3DES). The implementation uses the Java programming language. Text messages that are confidential and important in the form of SMS have a maximum encryption length (ciphertext) of 60 characters. The purpose of this research is to secure and maintain the confidentiality of information sent and received via SMS from theft and manipulation of data by unauthorized parties. The test results in this research show that the implementation of text cryptography with multiple encryptions using the RSA (Rivest Shamir Adleman) algorithm and 3DES (Triple Encryption Data Standard) in the SMS security application can secure text messages when sent and received by parties who have rights.

Keywords*— *text cryptography, multiple encryption, RSA algorithm, 3DES algorithm, SMS

Abstrak*— Layanan pesan singkat menjadi media komunikasi yang lebih banyak dipilih dibandingkan pesan suara. Saat ini masih banyak yang menggunakan SMS karena tidak memiliki hambatan *platform* ataupun teknologi, sehingga pengirimannya juga cepat. Jika menggunakan aplikasi pesan singkat, seperti Whatsapp, maka memerlukan koneksi internet. Pengiriman SMS memiliki informasi yang bersifat penting dan rahasia. Salah satu contohnya adalah pesan mengenai waktu dan tempat pelaksanaan penggerebekan narkoba atau perjudian. Masalahnya adalah keamanan informasi yang dikirimkan melalui SMS cukup rentan terhadap kebocoran informasi. Oleh karena itu, diperlukan aplikasi untuk mengamankan pesan teks tersebut agar tidak dapat dibaca oleh pihak yang tidak berkepentingan. Pengamanan tersebut menggunakan *multiple encryption* dengan algoritme kriptografi *Rivest Shamir Adleman (*RSA) dan *Triple Encryption Data Standard* (3DES). Implementasinya menggunakan bahasa pemrograman Java. Pesan teks yang bersifat rahasia dan penting dalam bentuk SMS memiliki panjang enkripsi (*ciphertext*) maksimal 60 karakter. Tujuan penelitian ini adalah mengamankan dan menjaga kerahasiaan informasi yang dikirim dan diterima melalui SMS dari terjadinya pencurian dan manipulasi data oleh pihak yang tidak berkepentingan. Hasil pengujian dalam penelitian ini membutikan bahwa implementasi kriptografi teks dengan *multiple encrypton* menggunakan algoritme RSA (*Rivest Shamir Adleman*) dan 3DES (*Triple Encryption Data Standard*) pada aplikasi pengamanan SMS dapat mengamankan pesan teks saat dikirim dan diterima oleh pihak yang memiliki hak.

***Kata Kunci*— kriptografi teks, *multiple encryption*, algoritme RSA, algoritme 3DES, SMS**

I. PENDAHULUAN

Tingkat kejahatan di DKI dari tahun 2016-2018 [1] menempati peringkat tinggi tingkat nasional mulai dari pembunuhan dengan persentase 5,24%, kejadian pencurian dengan kekerasan 14,23%, kejahatan penyalahgunaan dan peredaran narkoba 34,46%, dan masih banyak lagi. Lembaga negara yang bertugas menjaga keamanan, ketertiban, dan penegakan hukum yaitu Kepolisian Negara Republik Indonesia yang salah satunya berada pada komando kota/kabupaten yang disebut dengan kepolisian resor (Polres).

Polres Jakarta Selatan adalah salah satu kantor kepolisian yang bertanggung jawab atas keamanan warga di sekitar area Jakarta Selatan. Dalam melaksanakan salah satu kegiatannya, ada informasi rahasia mengenai waktu dan tempat pelaksanaan penggerebekan yang harus diinfokan oleh Kepala Polres Jakarta Selatan kepada jajarannya melalui fasilitas SMS. Informasi rahasia ini perlu diamankan agar tidak diketahui oleh pihak lain, tujuan dari pengamanan informasi ini menurut Paryati [2] adalah: (1) menjaga kerahasiaan sehingga hanya dapat diakses oleh pihak-pihak yang diotorisasi sehingga keutuhan serta konsistensi data pada sistem tetap terjaga; (2) ketersediaan yaitu menjamin pengguna yang sah untuk selalu dapat mengakses informasi

dan sumberdaya yang diotorisasi; (3) integritas yaitu menjamin konsistensi dan menjamin data tersebut sesuai dengan aslinya, sehingga upaya orang lain yang berusaha merubah data akan segera dapat diketahui; (4) penggunaan yang sah yaitu menjamin kepastian bahwa sumber daya tidak dapat digunakan oleh orang yang tidak berhak

Berdasarkan analisis masalah di atas maka diperlukan pengamanan pesan teks pada SMS dengan kriptografi teks yang bertujuan untuk mengamankan pesan teks saat dikirim dan diterima oleh pihak yang memiliki hak. Tempat studi kasus untuk mengimplementasikan pengamanan pesan ini adalah Polres Jakarta Selatan yang ingin melindungi pesan SMS dari pihak yang tidak berhak terutama oleh pihak yang akan diperiksa/digerebek sehingga tidak mengganggu pelaksanaan kegiatan dari Polres Jakarta Selatan. Pengamanan SMS pada aplikasi ini menggunakan kriptografi yang menurut Bruce [3] kriptografi merupakan suatu seni atau ilmu untuk menjaga kerahasiaan dari sebuah tulisan agar tetap aman, tanpa diketahui pihak yang tidak berkepentingan.

Penelitian tentang pengamanan pesan atau *file* dengan menggunakan kriptografi sudah banyak dilakukan, antara lain penelitian yang mengembangkan sebuah aplikasi pada *smartphone* berbasis Android untuk memodifikasi pesan SMS menjadi *ciphertext* agar isi informasi dari SMS tersebut tidak diketahui oleh orang lain menggunakan algoritme RSA [4]. Penelitian yang membuat aplikasi *desktop* dengan Java untuk mengamankan isi *e-mail* berupa *plaintext*, bukan *attachment file* [5]. Penelitian yang membangun sebuah aplikasi pesan instan pada perangkat Android dengan mengimplementasikan algoritme RSA dalam proses enkripsi dan dekripsi [6]. Penelitian yang membangun aplikasi berbasis *desktop* dengan bahasa pemrograman Visual Basic 6 untuk mengamankan *file* dokumen dengan algoritme RSA [7]. Penelitian yang membuat aplikasi berbasis *web* untuk mengamankan *file* rekam medik pada klinik Dr. H. Hartono yang dikirimkan menggunakan *e-mail* [8]. Penelitian aplikasi keamanan SMS menggunakan algoritme Triple-Des dan menguji serangan *man in the middle attact* (MITM) dengan menggunakan metode *sniffing* [9]. Penelitian yang menggunakan enkripsi berganda (*multiple encryption*) juga sudah banyak dilakukan dengan tujuan untuk meningkatkan keamanan data dan integritas data rahasia, serta memiliki keuntungan. Jika salah satu kunci direntas atau beberapa bagian dari teks kunci rusak, kerahasiaan dan privasi data asli masih dapat dipertahankan dengan enkripsi lainnya [10]. Penelitian [11] membuat metode untuk mengamankan data yang besar di internet dengan *multiple encryption* menggunakan algoritme AES, RSA, dan AESP. Kemudian mengembangkan metode untuk mengamankan semua data tersebut dengan cara membuat antrian melingkar, di mana ketiga algoritme tersebut akan melakukan enkripsi data bervolume besar secara bergantian. Metode ini dianggap lebih aman dan efektif.

Berdasarkan penelitian yang pernah dilakukan sebelumnya maka pada penelitian ini akan dilakukan pengamanan pesan teks dengan *multiple encryption* menggunakan 2 (dua) metode, yaitu RSA dan 3DES. Alasan digunakannya algoritme RSA adalah menurut Munir [12], RSA adalah algoritme kriptografi kunci publik yang paling populer dan memiliki keamanan yang terjamin dan menurut Ginting [13], sampai saat ini belum ada penyerangan terhadap RSA yang efektif jika pemilihan parameter dan implementasinya tepat terhadap RSA. Alasan penelitian ini menggabungkan RSA dengan pengamanan algoritme 3DES adalah karena algoritme 3DES adalah algoritme simetris yang digunakan untuk menyimpan pesan teks yang pada awalnya bernama algoritme DES [14]. Namun, algoritme DES dianggap sudah tidak aman lagi [15] karena kuncinya dapat ditemukan dalam waktu beberapa hari sehingga dikembangkan menjadi 3DES. Dalam prosesnya, algoritme DES diulang sebanyak 3 kali sehingga lebih aman.

Tujuan penelitian ini adalah merancang dan membangun aplikasi Pengamanan SMS untuk implementasi kriptografi teks menggunakan *multiple encryption* dengan algoritme RSA (*Rivest Shamir Adleman*) dan 3DES (*Triple Data Encryption Standard*) sehingga dapat mengamankan informasi yang bersifat privasi atau rahasia. Batasan masalah pada penelitian ini adalah aplikasi Pengamanan SMS hanya dapat digunakan pada sistem operasi Android dan panjang karakter pengiriman pesan dari aplikasi Pengamanan SMS yang akan dibuat adalah maksimal sebanyak 160 (seratus enam puluh) karakter pesan enkripsi (*ciphertext*).

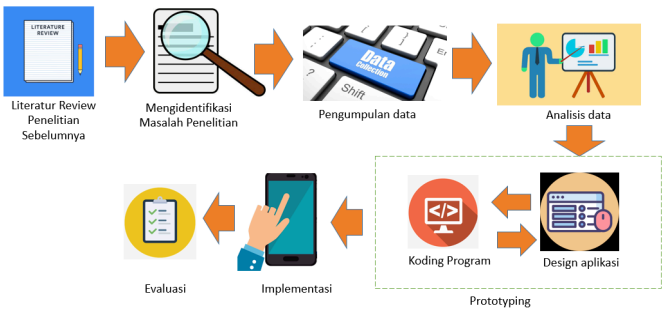
II. METODOLOGI

A. *Waktu dan Subjek Penelitian*

Waktu penelitian dilakukan pada bulan September 2018 – Januari 2019. Subjek penelitian adalah analisis kebutuhan pengguna dengan studi kasus di Polres Jakarta Selatan yang berlokasi di Jl. Wijaya 11 No. 42, Kebayoran, Jakarta Selatan, DKI Jakarta. Nomor Telepon 021-7206011.

B. *Desain Penelitian*

Gambar 1 menunjukkan tahapan yang dilakukan dalam penelitian ini. Tahapan penelitian pada Gambar 1 dimulai dengan studi literatur penelitian yang pernah dilakukan sebelumnya, berkaitan dengan topik kriptografi pada teks dan *multiple encryption*, kemudian identifikasi masalah penelitian yang berkaitan dengan proses pengamanan SMS, dan pengumpulan data di tempat studi kasus Polres Jakarta Selatan. Setelah data terkumpul, kemudian dilakukan analisis data dengan merancang arsitektur sistem. Proses selanjutnya, dilakukan rancang bangun aplikasi Pengamanan SMS dengan menggunakan metode pengembangan sistem *prototyping*,



Gambar 1 Tahapan penelitian

yaitu aktifitas pengembangan produk perangkat lunak yang sering digunakan saat ini. Karena perangkat lunak tidak berbentuk fisik, maka proses pengembangan prototipe yang berulang (beriterasi) dapat mendorong proses pengembangan dengan biaya pendekatan yang lebih efisien. Hal ini menjadikan pendekatan pembangunan aplikasi yang layak sesuai keinginan pengguna [16]. Kelebihan lain dari model *prototyping* ini adalah komitmen yang jelas antara pengembang, pengguna, dan pemimpin organisasi [17]. Pada tahap *prototyping* dilakukan desain aplikasi dan pemrograman berulang hingga pengguna merasa nyaman dengan aplikasi yang sedang dibangun. Setelah aplikasi selesai dibangun, maka tahap berikutnya adalah aplikasi diberikan kepada pengguna untuk dilakukan uji coba dan evaluasi.

Tahapan yang dilakukan pada metode *prototyping* yaitu melakukan pengumpulan data yang dibutuhkan untuk data penelitian. Data yang berhasil dikumpulkan, dianalisis dan dilakukan desain aplikasi. Setelah desain aplikasi, dilakukan pengkodean program sehingga menjadi *prototype* aplikasi. Kemudian meminta pengguna untuk memberikan respon terhadap *prototype*. Jika pengguna memberi respon belum sesuai maka peneliti akan merancang dan melakukan pemrograman sesuai respon pengguna. Setelah prototype sesuai, aplikasi dapat diimplementasikan di Polsek Jakarta Selatan. Dalam penelitian ini juga dilakukan evaluasi hasil penelitian.

C. Cara Kerja Algoritme RSA

Algoritme RSA dibuat oleh 3 orang peneliti dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman [12].

1) *Perumusan Kunci RSA*

- Pilih dua buah bilangan prima sembarang, p dan q.
- Hitung $n = p \cdot q$ (sebaiknya $p \neq q$, jika $p = q$ maka
- $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
- Hitung $\varphi(n) = (p - 1)(q - 1)$.
- Pilih kunci publik, e, yang relatif prima terhadap $\varphi(n)$.
- Bangkitkan kunci privat dengan menggunakan persamaan $e.d \equiv 1 \ (mod\ \varphi(n))$.

Perhatikan bahwa $e \cdot d \equiv 1 \ (mod\ \varphi\ (n))$ ekiuvalen dengan $e \cdot d = 1 + k\varphi(n)$, sehingga d dapat dihitung dengan:

$$d = \frac{1 + k\varphi\ (n)}{e} \qquad (1)$$

Terdapat bilangan bulat k yang memberikan bilangan bulat d. Hasil dari algoritme di atas:

- Kunci publik adalah pasangan (e, n)
- Kunci privat adalah pasangan (d, n)

2) *Metode Enkripsi*

Langkah-langkah dalam mengenkripsi pesan:

- Ambil kunci publik penerima pesan, e, dan modulus n.
- Nyatakan *plainteks m* menjadi blok-blok *m1*, *m2*,…, sedemikian sehingga setiap blok merepresentasikan nilai di dalam selang $[0, n - 1]$.
- Setiap blok m_i dienkripsi menjadi blok c_i dengan rumus:

$$C_i = m_i^e \bmod n \qquad (2)$$

3) *Metode Dekripsi*

- Setiap blok *ciphertext* c_i didekripsi kembali menjadi blok m_i dengan rumus:

$$m_i = C_i^d \bmod n \qquad (3)$$

D. Cara Kerja Algoritme 3DES

Metoda 3DES menggunakan DES sebanyak 3 kali. Bentuk sederhana perhitungan untuk enkripsi dan dekripsi 3DES adalah [14]:

Enkripsi:

$$C = EK3(EK2(EK1(P))) \qquad (4)$$

Penjelasannya, enkripsi pesan P dengan kunci *K1* lalu dengan kunci *K2*. Setelah itu, kembali dengan kunci *K3*. Hasil enkripsi terakhir adalah *chipherteks*

Dekripsi:

$$P = DK1(DK2(DK3(C))) \qquad (5)$$

Penjelasan, mula-mula kunci *K3* digunakan untuk mendekripsi *C*, lalu hasilnya dienkripsi lagi dengan kunci K2. Setelah itu, dideskripsi lagi dengan kunci *K1*. Hasil dekripsi terakhir adalah pesan semula (*P*).

Proses enkripsi sebanyak tiga kali, seperti yang diperlihatkan pada Gambar 2, sedangkan skema untuk dekripsinya diperlihatkan pada Gambar 3.

III. HASIL DAN PEMBAHASAN

A. Analisis Kebutuhan Aplikasi

Gambar 2 Enkripsi 3DES [14]

Gambar 3 Dekripsi 3DES [14]

Agar aplikasi Pengamanan SMS dapat berjalan dengan baik, maka diperlukan spesifikasi perangkat keras dan perangkat lunak yang akan digunakan saat implementasi, yaitu:

1) *Spesifikasi Perangkat Keras*

Perangkat keras yang digunakan untuk mendukung aplikasi ini secara maksimal, memiliki spesifikasi: *smartphone* berbasis Android, 1.2GHz Dual Core, dan RAM 1 GB.

2) *Spesifikasi Perangkat Lunak*

Spesifikasi Perangkat lunak yang digunakan oleh pengguna: Sistem Operasi Jelly Bean dan *browser*.

B. Arsitektur Sistem

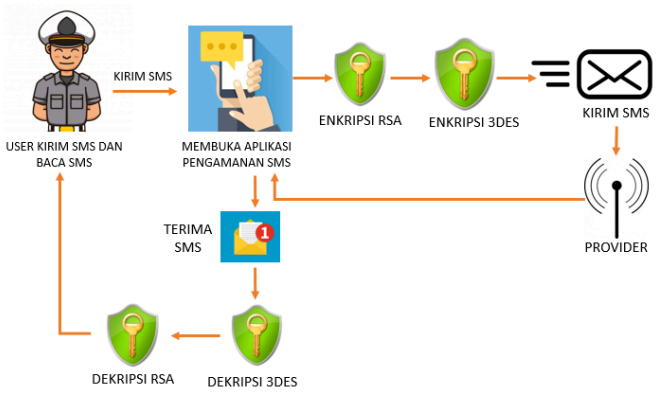
Pada Gambar 4 dapat dilihat arsitektur sistem pada aplikasi Pengamanan SMS, yaitu implementasi dari *multiple encryption* dengan metode RSA dan 3DES. Alur sistem dimulai dari pengguna mengirimkan pesan menggunakan aplikasi Pengamanan SMS kemudian pesan dienkripsi sehingga membentuk ciphertext dan dikirim. Penerima pesan akan membaca SMS melalui aplikasi pengamanan pesan dengan memasukkan kunci sehingga pesan berbentuk *plaintext* yang dapat dibaca oleh penerima yang berhak.

C. Alur Kerja Multiple Encryption RSA dan 3DES

Pada penelitian ini digunakan dua tahap enkripsi, yaitu enkripsi dengan algoritme RSA dan algoritme 3DES. Pengguna akan memasukkan pesan SMS dalam bentuk teks (*plaintext*) dan memasukkan kunci. Setelah itu, *plaintext* dan kunci akan dienkripsi dengan algoritme RSA. Proses ini akan menghasilkan *ciphertext* RSA yang akan dienkripsi kembali oleh 3DES sehingga menghasilkan *ciphertext* 3DES. Secara garis besar, alur enkripsi pada penelitian ini ditunjukkan pada *flowchart* pada Gambar 5.

D. Alur Kerja Dekripsi pada Aplikasi

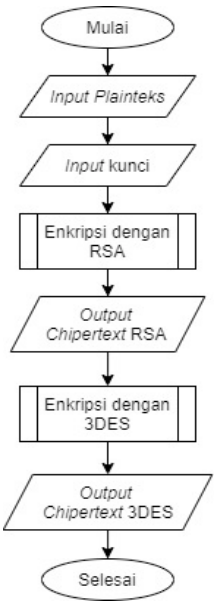
Alur kerja dekripsi dimulai saat pengguna mendapatkan pesan masuk. Jika pengguna ingin membaca isi pesan masuk, pesan tersebut masih berbentuk *ciphertext.* Untuk membaca isi pesan, pengguna memasukkan kunci, kemudian kunci tersebut akan digunakan untuk melakukan dekripsi. Tahap pertama, dilakukan dekripsi dengan algoritme 3DES dan dilakukan dekripsi dengan RSA sehingga menghasilkan *plaintext* yang dapat dibaca oleh penerima pesan teks. Secara garis besar, alur dekripsi pada penelitian ini ditunjukkan pada *flowchart* pada Gambar 6.



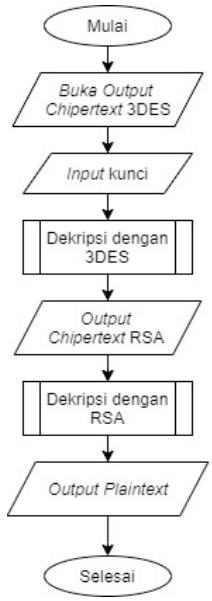
Gambar 4 Arsitektur sistem *Multiple Encryption* pada aplikasi pengamanan pesan singkat pada *platform* Android

E. Alur Proses Algoritme RSA pada Aplikasi

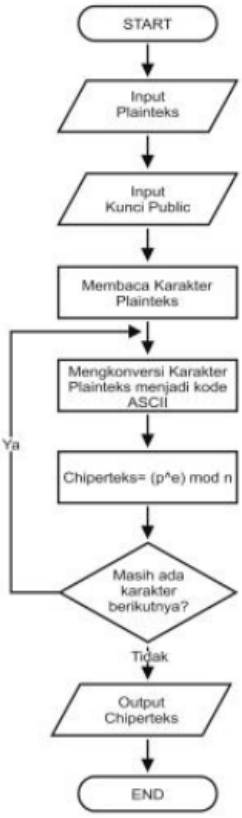
Aplikasi pengamanan pesan singkat yang menggunakan algoritme RSA memiliki alur proses penyandian data yang menggunakan kunci publik (*n,e*). Awalnya, data yang dimasukkan akan diubah ke dalam bentuk ASCII pada setiap karakternya. Selanjutnya, *plaintext* akan dienkripsikan menjadi *ciphertext*. Prosesnya dapat dilihat pada Gambar 7 [18].



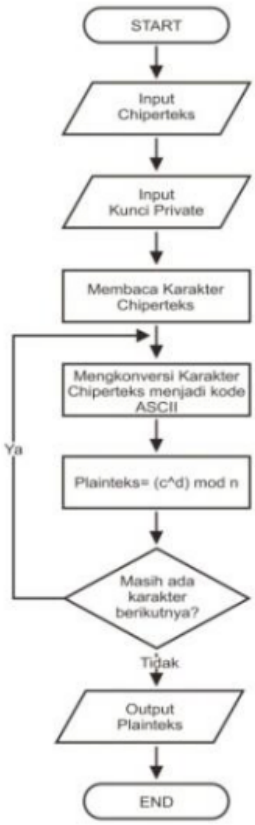
Gambar 5 Alur kerja enkripsi RSA dan 3DES pada aplikasi pengaman SMS



Gambar 6 Alur kerja dekripsi RSA dan 3DES pada aplikasi pengaman SMS



Gambar 7 *Flowchart* proses enkripsi RSA [18]



Gambar 8 Proses dekripsi algoritme RSA [18]

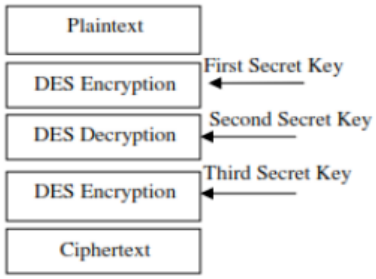
Dalam proses dekripsi, pengubahan data yang sudah disandikan (*ciphertext*) menggunakan kunci publik (*e,n*) menjadi pesan awal (*plaintext*) dapat dilakukan dengan menggunakan kunci *privat* (*d,n*). *Ciphertext* yang dimasukkan akan diubah ke dalam bentuk ASCII pada setiap karakternya. Selanjutnya, *ciphertext* akan didekripsikan menjadi *plaintext*. Prosesnya dapat dilihat pada Gambar 8 [18]. Kunci privat didapatkan dari pembangkit kunci yang diproses saat proses enkripsi. Kunci tersebut akan diberikan kepada penerima pesan jika ingin membuka pesan teks menggunakan aplikasi Pengamanan SMS.

F. Blok diagram Algoritme 3DES pada Aplikasi

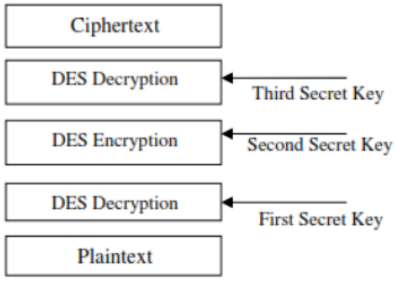
Alur proses algoritme 3DES memiliki alur proses DES enkripsi untuk kunci pertama, DES dekripsi untuk kunci kedua, dan DES enkripsi untuk kunci ketiga. Blok diagram enkripsi algoritme 3DES terdapat pada pada Gambar 9 dan blok diagram dekripsi algoritme 3DES pada Gambar 10.

G. Implementasi Multiple Encryption pada Aplikasi

Multiple encryption untuk kriptografi pesan dalam bentuk teks menggunakan algoritme RSA dan 3DES akan diimplementasikan ke dalam aplikasi Pengamanan SMS pada Polres Jakarta Selatan. Tampilan aplikasi yang akan disajikan pada penelitian ini adalah tampilan menu utama, tampilan isi pesan baru, dan tampilan isi pesan masuk. Gambar 11 memperlihatkan tampilan menu utama dari aplikasi yang menampilkan 4 fitur, yaitu: fitur Pesan Baru, Pesan Masuk, Pesan Keluar, dan Bantuan.



Gambar 9 Diagram blok enkripsi algoritme 3DES [19]



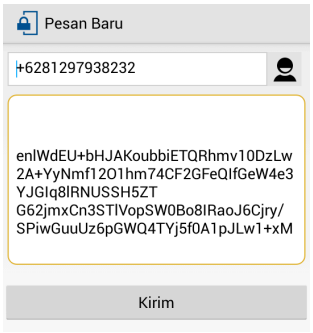
Gambar 10 Diagram blok dekripsi algoritme 3DES [19]

Jika pengguna memilih menu Pesan Baru pada aplikasi Pengamanan SMS (Gambar 11), maka akan muncul tampilan seperti pada Gambar 12. Pengirim pesan akan memasukkan nomor penerima pesan, lalu menulis isi pesan dalam bentuk

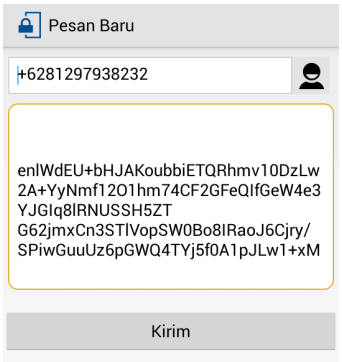
teks dan memasukkan kunci. Setelah yakin dengan isi pesan, maka pengirim pesan akan menekan tombol kunci sehingga akan tampil pesan yang terenkripsi, seperti terlihat pada Gambar 13. Pengirim pesan akan menekan tombol kirim lalu pesan teks akan terkirim ke penerima pesan.

Penerima pesan akan menerima pesan pada menu Pesan Masuk yang terdapat pada aplikasi Pengamanan SMS (Gambar 11). Penerima pesan membuka salah satu pesan dan akan tampil halaman Lihat Pesan, seperti pada Gambar 14. Pesan masih berbentuk *ciphertext* sehingga penerima pesan harus memasukkan kunci untuk mendekripsi pesan masuk agar dapat melihat pesan yang diterima, seperti diperlihatkan pada Gambar 14.

Gambar 11 Tampilan nenu utama dari aplikasi pengamanan pesan singkat



Gambar 12 Tampilan menu Pesan Baru dari aplikasi Pengamanan SMS



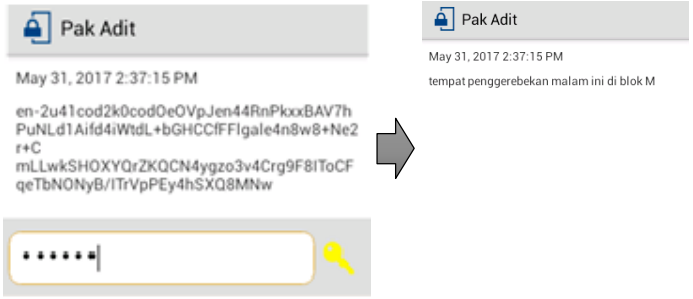
Gambar 13 Tampilan Pesan Terkirim yang telah dienkripsi dari aplikasi Pengamanan SMS

H. Pengujian Proses Pengamanan Pesan Teks

Pada tahap pengujian, akan dibahas akurasi proses enkripsi dan dekripsi pesan dalam bentuk teks menggunakan aplikasi Pengamanan SMS. Tahapan pengujiannya yaitu pesan asli diproses menggunakan *multiple encyrption* dengan metode RSA dan 3DES menjadi *ciphertext,* kemudian pesan *ciphertext* dikirim dan dibuka kembali oleh aplikasi juga dengan menggunakan *multiple encryption*.

Tabel I menampilkan hasil uji coba enkripsi pesan teks melalui aplikasi Pengamanan SMS. Isi pesan asli yang memiliki panjang karakter sedikit, ketika diubah menjadi *ciphertext*, memiliki panjang karakter 3 kali lebih besar dari pesan asli. Hal tersebut karena *ciphertext* merupakan hasil dari kombinasi *plaintext* dan kunci.

Tabel II menampilkan hasil uji coba dekripsi pesan teks melalui aplikasi Pengamanan SMS. Isi pesan *ciphertext* yang memiliki panjang karakter 3 kali lebih besar dari pesan asli, saat diproses dengan *multiple encryption*, maka berubah menjadi pesan asli yang memiliki panjang karakter 1/3 kali lebih kecil dari *ciphertext*.



Gambar 14 Tampilan Pesan Masuk yang terdekripsi dari aplikasi Pengamanan SMS

TABEL I
PERCOBAAN ENKRIPSI PESAN SINGKAT DENGAN *MULTIPLE ENCRYPTION* ALGORITME RSA DAN 3DES

Isi pesan asli (*plaintext*)	**Panjang karakter *plaintext***	**Isi pesan enkripsi (*ciphertext*)**	**Panjang karakter *ciphertext***
Tempat penggerebekan malam ini di Blok M	40	En-2u41cod2k0codOeOVpJen44RnPkxx BAV7hPuNLd1Aifd4iWtdl +bGHCCfFFlgAle4n8w8+1 e2r+CmLLwkSHOXYQrZl QCN4ygzo3v4Crg9F8IToC qeTbNONyB/ItrVpPEy4hS Q8MNw	143
Waktu penggerebekan malam ini pukul 22:00 WIB	45	P9jBqBfHJuxB+iBtmGvs9l QNOduoiNtYq5eAEAb5ou WoFHCjRnCZqTgulEr8 2Z7lc4V+Weaq/TNv31gmc ToHnjYew4RpgyEbqROzX LXDDTKz5eC+YcTdEpFl uB7ot34LVdG4kSk3U	139

Dari Tabel I dan Tabel II dapat disimpulkan bahwa implementasi *multiple encryption* dengan algoritme RSA dan 3DES pada aplikasi pengaman SMS terbukti dapat menyembunyikan isi pesan dalam bentuk teks ke dalam bentuk *ciphertext*. Isi pesan menjadi aman dari pihak-pihak yang tidak memiliki hak terhadap informasi tersebut. Pesan *ciphertext* tersebut dapat dikembalikan ke bentuk pesan asli (*plaintext*) sehingga dapat dibaca oleh penerima pesan teks yang memiliki hak akses.

I. Evaluasi Program

Aplikasi Pengamanan SMS diuji coba oleh 10 (sepuluh) orang responden. Aplikasi Pengamanan SMS diuji coba dengan cara menjawab pertanyaan pada kuesioner sebagai bentuk evaluasi. Tabel III menampilkan hasil kuesioner yang diberikan kepada 10 orang responden tersebut beserta penilaiannya terhadap aplikasi Pengamanan SMS.

Tanggapan responden yang bernilai baik untuk semua pertanyaan pada kuesioner ditampilkan pada Gambar 15.

Kekurangan pada aplikasi Pengamanan SMS ini adalah aplikasi ini tidak memiliki fitur *broadcast* untuk mengirimkan pesan yang sama ke semua kontak pengguna dalam sekali pengiriman. Aplikasi ini pun tidak dapat menghapus banyak pesan sekaligus.

TABEL II
PERCOBAAN DEKRIPSI PESAN SINGKAT DENGAN *MULTIPLE ENCRYPTION* ALGORITME RSA DAN 3DES

Isi pesan enkripsi (*ciphertext*)	**Panjang karakter pesan enkripsi**	**isi pesan dekripsi/asli (*plaintext*)**	**Panjang karakter pesan dekripsi**
En-2u41cod2k0codOeOVpJen44RnPkxxBAV7hPuNLd1Aifd4iWtdL+bGHCCfFFlgAle4n8w8+Ne2r+CmLLwkSHOXYQrZKQCN4ygzo3v4Crg9F8IToCFqeTbNONyB/ItrVpPEy4hSXQ8MNw	143	Tempat penggerebekan malam ini di Blok M	40
P9jBqBfHJuxB+iBtmGvs9bQNOduoiNtYq5eAEAb5oujWoFHCjRnCZqTgulEr82Z7lc4V+Weaq/TNv31gmcToHnjYew4RpgyEbqROzXLXDDTKz5eC+YcTdEpFliuB7ot34LVdG4kSk3U	139	Waktu penggerebekan malam ini pukul 22:00 WIB	45

IV. SIMPULAN

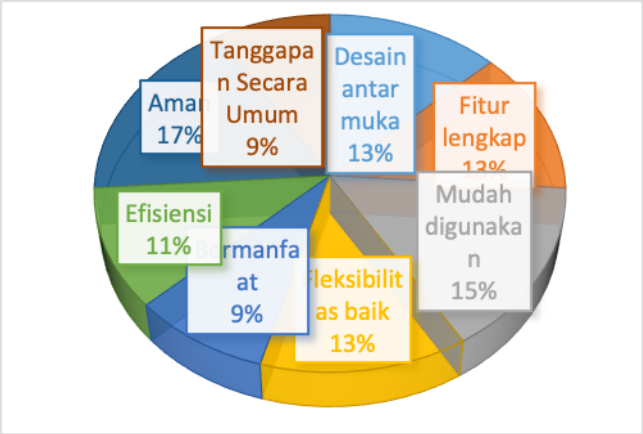
Kesimpulan dari penelitian ini adalah implementasi kriptografi teks dengan *multiple encrypton* menggunakan algoritme RSA (*Rivest Shamir Adleman*) dan 3DES (*Triple Encryption Data Standard*) pada aplikasi Pengamanan SMS setelah diuji dapat mengamankan pesan teks saat dikirim dan diterima oleh pihak yang memiliki hak. Pesan teks yang sudah dienkripsi dapat dikembalikan (dekripsi) menjadi data semula tanpa ada perubahan sehingga informasi yang bersifat rahasia dapat dikirimkan dan diterima dengan aman.

UCAPAN TERIMA-KASIH

Terima kasih disampaikan kepada Universitas Budi Luhur yang telah memberikan bantuan hibah internal sehingga terlaksana penelitian ini, dan terima kasih kepada Kepolisian Reosr (Polres) Jakarta Selatan dan jajarannya yang telah bersedia menjadi narasumber dari penelitian ini.

TABEL III
HASIL PENGOLAHAN DATA KUESIONER PENGGUNA APLIKASI PENGAMANAN SMS MENGGUNAKAN *MULTIPLE ENCRYPTON*

Pertanyaan Kuesioner tentang Aplikasi	**Tanggapan Responden**			
	sangat baik	**baik**	**cukup baik**	**kurang baik**
Desain antar muka	0	6	4	0
Fitur lengkap	2	6	2	0
Mudah digunakan	2	7	1	0
Fleksibilitas baik	1	6	3	0
Bermanfaat	3	4	3	0
Efisiensi	2	5	3	0
Aman	1	8	1	0
Tanggapan secara umum	3	4	3	0



Gambar 15 Tanggapan responden bernilai baik pada semua pertanyaan kuesioner

DAFTAR REFERENSI

[1] Badan Pusat Statistik, *Statistik Kriminal 2018*. Jakarta: Badan Pusat Statistik, 2018.

[2] Paryati, "Keamanan sistem informasi," dalam *Seminar Nasional Informatika 2008 (Semnasif 2008)*, UPN Veteran, Yogyakarta, 24 Mei 2008, hlm. 379–386.

[3] B. Schneier, *Applied Cryptography: Protocols, Algorithms and Source Code in C*, 2nd ed. Wiley, 2015.

[4] A. R. Alvianto dan D. Darmaji, "Pengaman pengiriman pesan *via* SMS dengan algoritme RSA berbasis Android," *J. Sains dan Seni ITS*, vol. 4, no. 1, hlm. 1–5, 2015.

[5] A. Ginting, R. R. Isnanto, dan I. P. Windasari, "Implementasi algoritme kriptografi RSA untuk enkripsi dan dekripsi *email*," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, hlm. 253, 2015.

[6] M. A. Zainuddin dan D. I. Mulyana, "Penerapan algoritme RSA untuk keamanan pesan instan pada perangkat Android," *J. CKI on Spot*, vol. 9, no. 2, hlm. 105–114, 2016.

[7] P. Pahrizal dan D. Pratama, "Implementasi algoritme RSA untuk pengamanan data berbentuk teks," *J. Pseudocode*, vol. 3, no. 1, hlm. 44–49, 2016.

[8] D. Anggraini dan S. Juanita, "Aplikasi *e*-arsip pengamanan pesan elektronik berbasis *web* dengan mengimplementasikan algoritme kriptografi RSA dan *ElGamal* pada Klinik Dr. H. Hartono," *J. Ticom*, vol. 6, no. 3, hlm. 122–130, 2018.

[9] S. W. Wardani, Sutardi, dan Statiswaty, "Aplikasi keamanan SMS menggunakan Triple-Des dan pengujian serangan *Man In The Middle Attact* (*MITM*) dengan metode *sniffing*," *SemanTIK*, vol. 5, no. 1, hlm. 113–120, 2019.

[10] H. Gupta dan V. K. Sharma, "Role of multiple encryption in secure electronic transaction," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 6, hlm. 89–96, 2011.

[11] K. K. Jabbar, H. A. Hilal, dan R. S. Mohammed, "Text cryptography using multiple encryption algorithms based on circular queue via cloud computing environment," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 12, hlm. 3654–3663, 2018.

[12] R. Munir. IF-5054. Diktat Kuliah. Topik: "Kriptografi: algoritme RSA dan ElGamal," Departemen Teknologi Informatika, Institut Teknologi Bandung, 2004.

[13] N. F. Ginting dan M. Ginting, "Perbandingan kriptografi RSA dengan Base64," *J. Tek. Inform. Unika St. Thomas*, vol. 2, no. 2, hlm. 47–52, 2017.

[14] E. Apulina dan G. N. Setiawan, "Perbandingan metode modifikasi 3DES dengan metode 3DES" *Telematika*, vol. 7, no. 1, hlm. 3–6, 2011.

[15] N. Siregar, "Perancangan aplikasi keamanan pesan teks dengan menggunakan algoritme Triple-DES," *J. Tek. Inform. Kaputama*, vol. 3, no. 2, hlm. 11–17, 2019.

[16] C. W. Elverum, T. Welo, dan S. Tronvoll, "Prototyping in new product development: strategy considerations," dalam *Procedia CIRP*, 2016, vol. 50, hlm. 117–122.

[17] A. Susanto dan Meiryani, "System development method with the prototype method," *International Journal of Scientific & Technology Research*, 2019, vol. 8, no. 7, hlm. 141–144.

[18] D. Apdilah dan H. Swanda, "Penerapan kriptografi RSA dalam mengamankan *file* teks berbasis PHP," *J. Teknol. Inf.*, vol. 2, no. 1, hlm. 45, 2018.

[19] K. S dan M. A, "Data encryption and decryption by using Triple-DES and performance analysis of crypto system," *Int. J. Sci. Eng. Res.*, vol. 2, no. 11, hlm. 24–31, 2014.

Suci Indah Febriani, kelahiran Jakarta. Penulis menyelesaikan jenjang pendidikan Sarjana Teknik Informatika di Universitas Budi Luhur.

Safitri Juanita, kelahiran Tangerang. Penulis menyelesaikan jenjang pendidikan Magister di Universitas Indonesia. Aktifitas sehari-hari penulis sebagai dosen Program Studi Sistem Informasi Universitas Budi Luhur.

Mardi Hardjianto, kelahiran Jakarta. Penulis menyelesaikan jenjang pendidikan Doktoral di Universitas Gajah Mada.